PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, 9/08 — A1

(11) International Publication Number: **WO 98/37661**

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/US98/02839

(22) International Filing Date: 17 February 1998 (17.02.98)

(30) Priority Data:
08/802,070 19 February 1997 (19.02.97) US

(71) Applicant: U.S. ROBOTICS MOBILE COMMUNICATIONS CORP. [US/US]; 605 Norht 5600 West, P.O. Box 10620, Salt Lake City, UT 84116-0020 (US).

(72) Inventor: KETCHAM, Carl; 2947 West Ryan Drive, Taylorsville, UT 84118 (US).

(74) Agents: KRIEGER, Michael, F. et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

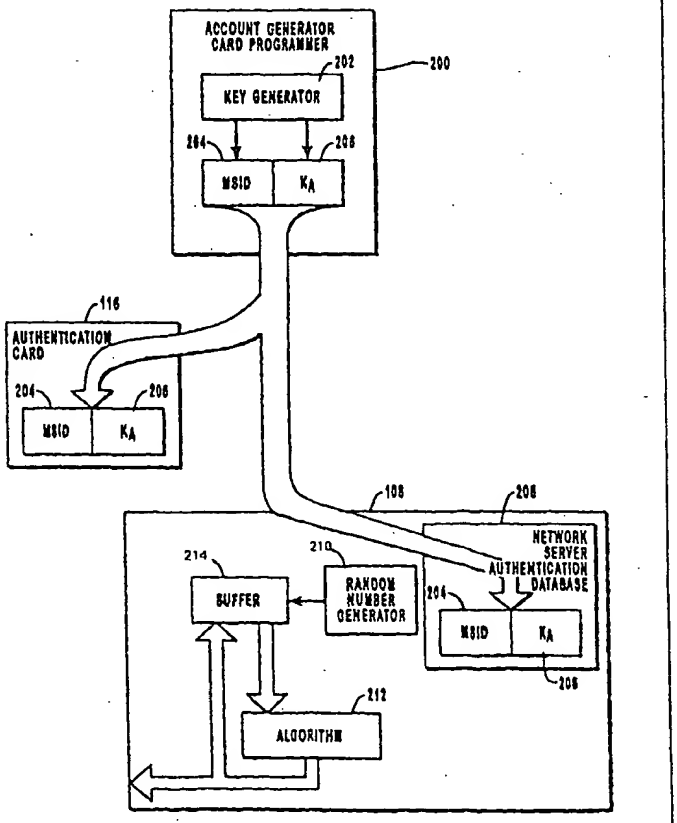
(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS AND METHOD FOR AUTHENTIFICATION AND ENCRYPTION OF A REMOTE TERMINAL OVER A WIRELESS LINK

(57) Abstract

A method and system for authenticating an authorized user of remote terminal (102) attempting to interconnect with computer network (104) over a wireless modem is provided. An encrypted wireless communication channel is established between remote terminal (102) and network server (108) for facilitating the authentication process. An authorized user present authentication card (118) containing credentials including a user identifier and authentication encryption key (206) to remote terminal (102). Remote terminal (102) establishes wireless communication channel (114) with network server (108) which provides a firewall between unauthenticated users and computer network (104). Network server (108) and remote terminal (102) then exchange encrypted information thus verifying the authenticity of each party. Remote terminal (102) and network server (108) each independently generate data encryption key (206) for use in establishing secure encrypted wireless communication channel (114) therebetween.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

APPARATUS AND METHOD FOR AUTHENTIFICATION AND ENCRYPTION OF A REMOTE TERMINAL OVER A WIRELESS LINK

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The field of the invention relates to computer and communication networks having a remote terminal isolated from the remainder of the computer network. More specifically, the present invention relates to verification of the identity of a user of the remote terminal, and more particularly, the invention relates to authenticating the user of the remote terminal as an authorized user of the computer network.

2. Present State of the Art

Computer networks have traditionally relied upon physical boundaries such as structures and facilities to provide security for the computer network. In fact, traditional networks interconnect computers or local terminals into networks using hard-wired physical connections for promoting interoperability. As such, local networks originally did not discriminate among users of the local terminals. As security awareness increased, local terminals provided discrimination by incorporating simplistic password protection. Because of the localized nature of password protection on a particular local terminal, users were often hindered from utilizing various other terminals.

As computer networks became more sophisticated additional resources were configured within the computer network to provide additional functionality such as extended data storage and centralized log-in protection. For example, as network servers became more sophisticated, authorized users of a computer network were able to migrate throughout the computer network to other local terminals. As computer network terminals increased in size and complexity security concerns also increased. One previous solution for managing such security concerns included interconnecting local smaller computer networks with other computer networks by physically coupling together network servers of each computer network. The coupling of these computer networks was generally accomplished using physical links such as coaxial cable or fiber optic lines. As computer networks became more diverse and spatially separated, security concerns were again raised that information exchanged between these intercomputer network links may become vulnerable to tampering or interception as such intercomputer network links often occur over public telephone lines or other accessible communication channels. To combat these concerns, network servers incorporated encryption protection for the information exchanged between computer networks. Encryption of exchange data

requires that each network server have a key or password for encrypting and decrypting exchanged information.

Furthermore, additional security concerns arise when local terminals within a computer network are no longer physically secured within a structural boundary. Such concerns arise when local terminals are remotely operated. Remote operation of a terminal raises an additional security concern regarding the authentication of the remote terminal. Some security concerns of remote operation of local terminals have been resolved by incorporating similar log-in password protection techniques for remote terminal operation as were required for local terminal operation. In such configurations, remote terminals are programmed with an identifier which may be verified by a network server as being a remote terminal authorized to operate within the computer network.

Additionally, prior configurations further protect informational exchanges between remote terminals and a network server by incorporating encryption into each informational exchange. Such bi-directional encryption required the pre-placement of matching encryption keys within both the remote terminal and the network server. Compatible informational exchange between the remote terminal and network server verified the identity of the remote terminal. Although such correlation of a remote terminal with a network server provides a level of assurance of the legitimacy of the remote terminal, the association of the encryption key with a remote terminal does not provide assurances to the network server of the identity of the user of the remote terminal. Resolution of this concern was mitigated by employing simplistic log-in password procedures. However, identification procedures incorporating users specific information stored on the remote terminal do not facilitate a particular remote user moving between remote terminals.

Mobile remote terminals present yet another variable to a computer network attempting to identify or authenticate legitimate users when such remote terminals attempt to access the computer network using wireless communication means. Such unpredictable remote access removes any physical benefits fixed site remote terminals may have provided since wireless communication channels may be established from non-fixed locations. Furthermore, as remote terminals employing wireless communication channels become more prevalent, they are becoming more fungible as access centers to computer networks. The security focus must then shift from authenticating an authorized remote terminal to focusing on authenticating the user of the remote terminal. Thus, prior art configurations have focused on authentication of a remote terminal optionally coupled with simplistic password protection of the remote

terminal against unauthorized users of the remote terminal rather than on authenticating the user themselves.

In conclusion, there exists a need for an apparatus and method for authenticating an authorized user prior to permitting access to a computer network. Furthermore, there exists a need for providing a method and system for establishing an encrypted authenticated wireless communication channel between an authorized user and a computer network. Though attempts have been made to correlate a remote terminal with authorized terminals of a computer network, there exists no scheme or configuration for solely authenticating an authorized user of a remote terminal and establishing an authenticated encrypted secure wireless communication channel therebetween.

SUMMARY OF THE INVENTION

The present invention authenticates an authorized user of a remote terminal in a computer network prior to permitting access of that authorized user to the computer network.

The present invention establishes a secure authenticated wireless communication channel between an authorized user of a remote terminal and a computer network.

The present invention provides a system for authenticating an authorized user of a computer network prior to permitting access of the authorized user to the computer network.

Furthermore, the present invention provides a system for establishing an encrypted authenticated wireless communication channel between a remote terminal and a computer network.

Additional advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims.

To achieve the foregoing, and in accordance with the invention as embodied and broadly described herein, an apparatus and method for authenticating an authorized user of a computer network which permits remote access by authorized users over a wireless communication channel is presented. Additionally, an apparatus and method for establishing a secure authenticated wireless communication channel is presented.

The present invention identifies an authorized user of the computer network and using encryption algorithmic techniques generates an authentication encryption key unique to that authorized user. The generation of the authentication encryption key and its association with a mobile subscriber identifier designating the authorized user are

generated and associated by an account generator within the system. The account generator, for example, may be a software application executing in conjunction with a computer or resident within a network server. The mobile subscriber identifier designating the authorized user coupled with the authenticating encryption key unique to that user are then securely distributed to both a network server coupled to a computer network and an authentication card to be securely carried by the authorized user.

The network server operates as a barrier or a firewall between the communication network and remote users attempting to access the computer network. As users attempt to access the computer network, the network server authenticates the user to determine if they are in fact a known authorized user. Authentication occurs over an unencrypted wireless communication channel wherein information is generated, manipulated, and mutually exchanged between the network server and the remote terminal. Each side independently verifies the other as being an authentic prior to continuing additional informational exchange. Furthermore, in the preferred embodiment, the remote terminal and the network server generate identical encryption keys for use in securing subsequent informational exchanges.

One exemplary embodiment of the present invention employs the remote terminal (e.g., a portable computer) operably coupled to a wireless modem for facilitating the establishment of a wireless communication channel. The remote terminal then initiates a communication request to the wireless modem to establish a communication channel with the network server. Once the communication channel is established, the network server prevents any access to other portions of the computer network prior to the successful completion of the authentication process.

To facilitate the authentication process both the authorized user and the network server must possess compatible mobile subscriber identifiers and authentication encryption keys. The network server maintains these values in a resident database. The remote terminal, however, does not retain the mobile subscriber identifier nor the authentication encryption key. Instead, an authentication card personal to the authorized user is maintained by that authorized user. The authorized user when desiring to establish an encrypted authenticated wireless communication channel with the network server inserts or places the authentication card in a card reader which is operably coupled to the remote terminal. The remote terminal then queries the authentication card via the card reader to extract the mobile subscriber identifier and its corresponding authentication encryption key. The remote terminal then dispatches the mobile subscriber identifier to the network server for use as an index in retrieving the corresponding authentication encryption key. The network server and remote terminal then commence in

authenticating the authorized user by exchanging, encrypting or signing information and then verifying the exchanged information to establish the authenticity of the user. In the preferred embodiment, when the users authenticity is established both the network server and the remote terminal independently generate a data encryption key for encrypting subsequent informational exchanges.

In the exemplary embodiment of the present invention, the network server initiates the mutual exchange of encrypted values by generating a random number. Upon receipt of this random number. the remote terminal employs encryption algorithms in conjunction with the authentication encryption key previously retrieved from the authentication card to sign or encrypt the random number. This signature of the remote terminal on the random number is then dispatched to the network server for verification. Upon successful verification of the signed random number, the network server demonstrates its authenticity by encrypting or signing and returning to the remote terminal the random number as previously signed by the remote terminal. The remote terminal upon successful verification of the network servers authenticity generates a data encryption key for subsequent informational exchanges with the network server. The network server, likewise, generates a data encryption key for corresponding communications with the remote terminal.

These and other features of the present invention will be more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth herein.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above recited and other advantages of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 is a block diagram of a system configured with a remote terminal capable of authenticating an authorized user of a computer network, in accordance with a preferred embodiment of the present invention.

Figure 2 is a functional block diagram depicting the generation, distribution, and processing of authentication keys, in accordance with one embodiment of the present invention.

Figure 3 is a functional block diagram of authentication key generation and distribution. in accordance with another embodiment of the present invention.

Figure 4 is a diagram of an authentication card associated with an authorized user for storage and presentation of authorized user-specific information, in accordance with an embodiment of the present invention.

Figure 5 is an authentication and encryption procedural diagram, in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As used herein, the term "remote terminal" refers to any known interfacing device such as a personal computer, notebook computer, or other mobile computer-type interfaces. Such "remote terminals" may be autonomous devices such as personal computers capable of independent functionality, or there may be simplified devices possessing minimal computation capabilities and thus primarily configured to receive and display information. This use of the term "remote terminal" is shown by way of example and not by limitation and those skilled in the art will undoubtedly understand and appreciate various different computational devices that are equally within the contemplation of the use of the term.

As used herein, the term "network server" refers to a peripheral system coupled within a computer network for providing and accommodating access to the network from diverse locations. Such an access point forms a barrier or a firewall to the remaining computer network. This use of the term "network server" is employed by way of example and those skilled in the art may also know of other interfacing mechanisms that are also contemplated within the scope of the present invention.

Figure 1 is a functional block diagram of a system 100 for authenticating an authorized user of a remote terminal prior to permitting access of the authorized user to the computer network. A computer network 104 is comprised of a plurality of local terminals 106 physically and operably coupled for beneficial processing. The coupling of local terminals 106 may be accomplished by traditional methods employed by local area networks or other networking techniques known by those of skill in the art. A network server 108 operably couples with computer network 104 for providing an access point to computer network 104. Network server 108 optionally may comprise additional support functionality for local terminals 106 such as remote disk servers for file storage.

Network server 108 additionally performs the function of providing a "firewall" for computer network 104. Network firewalls make it more difficult for computer networks to be infiltrated thus reducing or stopping malicious damage or intrusion. Network server 108 essentially places a barrier between computer network 104 and the

outside world. Network server 108 accommodates access by outside users to the verification and authentication processes of network server 108 prior to affording users outside of computer network 104 access within. Computer network 104 may be configured as a local area network or other area networks known by those skilled in the art such as wide area networks or other configurations.

As discussed above, users of computer networks frequently require access to networks from remote locations. To facilitate remote operation, a remote terminal 102 provides an interface to an authorized user similar or equivalent to those interfaces provided by local terminals. Furthermore, remote terminals may be sufficiently remote or mobile that a hardwire interconnect with computer network 104 is prohibitive. Thus, to facilitate interaction with computer network 104, a wireless communication channel 114 is established. Wireless communication channel 114, in the preferred embodiment, utilizes a wireless infrastructure 112 for interfacing to network server 108. Such wireless infrastructures may take the form of conventional cellular technologies such as analog and digital cellular. Analog cellular, such as AMPS, accommodate the transmission of digital information using traditional modem technology. Digital cellular, on the other hand, provides more diverse standards and more efficiently accommodates digital transmissions. Digital cellular standards such as USDC, GSM, and PCS transmit information over wireless communication channel 114 in digital form. Furthermore, some cellular standards also support collateral channels dedicated to the transmission of digital data. One such example is cellular digital packet data (CDPD) which facilitates the transmission and reception of intermittent packet data. Standard voice cellular channels require the establishment of a dedicated communication channel that is maintained throughout the entire communication session. However, CDPD facilitates sporadic data transmission be a plurality of dispersed digital transceivers without requiring each transceiver to establish and sustain a dedicated communication channel. A wireless modem 110 operably couples with remote terminal 102 for providing and facilitating the generation of wireless communication 114. Wireless modem 110 in the preferred embodiment, is capable of transmission and reception of CDPD information.

Card reader 116 operably couples with remote terminal 102 for providing an interface for receiving mobile subscriber identifiers and authentication keys from an authentication card 118. Card reader 116 may be physically integrated into remote terminal 102 or may be coupled to or integrated with wireless modem 110. Card reader 116 operably couples with an interface such as PCMCIA of remote terminal 102 for receiving control signals and providing data as requested by remote terminal 102.

Authentication card 118 provides a portable storage device for information specific to an authorized user. Such information includes a mobile subscriber identifier which designates the assigned identity of an authorized user and an authentication encryption key used to securely authenticate an authorized user and generate a data encryption key for providing encrypted secure data transmission over wireless communication channel 114.

Figure 2 is a functional block diagram depicting the generation, distribution, and processing of authentication keys in accordance with one embodiment of the present invention. An account generator 200 processes requests by authorized users for the generation of an authorized entry into network server 108 to facilitate a remote connection to a communication network by the authorized user. Account generator 200 comprises a key generator 202 receptive to an authorization request for generation of a cryptographically suitable authentication encryption key 206. Key generator 202 generates authentication encryption key 206 in accordance with parameters established by the cryptographic algorithm employed by both remote terminal 102 and network server 108 and by authentication card 118 and network server 108 in an alternative embodiment where authentication card 118 executes the cryptographic algorithm. In the preferred embodiment, a symmetric encryption algorithm is employed and those skilled in the art will appreciate that symmetric encryption algorithms employ the same encryption key for both encryption and decryption. However, the utilization of asymmetrical encryption algorithms such as RSA, are within the contemplation of the present invention. Asymmetrical encryption slightly increases the complexity of key generation and distribution by requiring the generation and distribution of an encryption key pair, one for encryption and a separate for decryption.

A mobile subscriber identifier 204 (MSID) is a numeric string designating a specific identity of an authorized user. Account generator 200 assimilates MSID 204 with authentication encryption key 206 thus providing an indexing designator for use by network server 108 in distinguishing among a plurality of authentication encryption keys 206. Account generator 200 disseminates MSID 204 coupled with authentication encryption key 206 to both an authentication card 116 and to network server 108. In Figure 2, account generator 200 is illustrated as being functionally separate from network server 108, however, nothing prevents account generator 200 from being physically associated with network server 108. Furthermore, in Figure 2, account generator 200 may also possess functionality for accommodating the programming of MSID 204 and authentication encryption key 206 into authentication card 116.

Network server 108 is further comprised of a network server authentication database 208 for receiving and storing MSID 204 and authentication encryption key 206. As network server 108 may accommodate plurality of mobile authorized users, network server authentication data base 208 may be comprised of a plurality of entries for multiple authorized users each having a unique MSID 204 and a corresponding authentication encryption key 206. In the preferred embodiment, network server 108 is also comprised of a random number generator 210 employed during the authentication process for generating a pseudo-random number. As will be detailed in Figure 5, a random number is employed during the authentication process of an authorized user with network server 108. Network server 108 further comprises functional elements such as algorithm 212 and buffer 214 for accommodating the authentication process.

Figure 3 is a functional block diagram of authentication key generation and distribution, in accordance with another embodiment of the present invention. The processing required by the network server 108' may be minimized by incorporating additional functionality into account generator 200'. In the present embodiment, account generator 200' generates or computes additional intermediate products or values for exchanging with remote terminal 102 (Figure 1). Such intermediate terms are then distributed to network server 108' for storage and retrieval during the authentication process. In the present embodiment, account generator 200' comprises key generator 202 for providing the general functionality of generating an authentication encryption key 206 and associating such a key with MSID 204 as detailed in Figure 2. Account generator 200' further comprises a random number generator 210 for generating a pseudo random number 302. As introduced in the description of Figure 2 and to be further described in Figure 5, random number 302 contributes to the authentication process. Algorithm 212 employs authentication key 206 and random number 302 to generate an authentication response 304. Authentication response 304 is further encrypted using authentication encryption key 206 and algorithm 212 to form a mobile authentication response 306, which is yet further encrypted using authentication encryption key 206 and algorithm 212 to form a data encryption key 308.

Account generator 200' then distributes mobile subscriber unit MSID 204, random number 302, authentication response 304, mobile authentication response 306, and data encryption key 308 to network server 108' for storage in network server authentication data base 208'. In the present embodiment, it is not necessary to distribute authentication encryption key 206 to network server 108' since account generator 200' has previously generated the intermediate terms necessary for verifying an authorized user. Furthermore,

account generator 200' has additionally generated data encryption key 308 for use in transmitting encrypted data between remote terminal 102 and network server 108'.

Although this present embodiment minimizes the required functionality of network server 108', it is, however, deemed some what less secure because of the inability of network server 108' to generate a unique data encryption key for subsequent sessions with remote terminal 102.

Figure 4 is a diagram of an authentication card associated with an authorized user for storage and presentation of authorized user-specific information, in accordance with an embodiment of the present invention. Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences.

Authentication card 118 is a portable storage device such as a smart card that may be conveniently transported by an authorized user to a remote terminal. In the preferred embodiment, authentication card 118 takes the form of a GSM subscriber identity module (SIM). A GSM SIM card has been utilized by GSM cellular communication systems for delivery of user identification details such as an international mobile subscriber identity (IMSI) and an authentication encryption key. It should be noted that nothing in the present invention prohibits a GSM SIM card from being employed to function as authentication card 118. As shown in Figure 4, when a GSM SIM card is employed, additional informational elements such as preferred networks 406, speed dial preferences 408, and short messages 410 may additionally be present within authentication card 118. Information may be extracted from authentication card 118 via interface 414 when authentication card 118 interfaces to card reader 116 (Figure 1).

As mentioned above, authentication card 118 may be implemented using smart card technology wherein a microprocessor, with typically 8 kbytes of memory, is based on a silicon chip and is embodied in a credit card sized package, however, nothing requires that authentication card 118 necessarily assume such a configuration. Furthermore, integration or minimization of authentication card 118 with temporary integration into a card reader 116 (Figure 1).

Figure 5 is an authentication and data encryption key-generation procedural diagram, in accordance with the preferred embodiment of the present invention. The authentication process commences with a user 101 approaching or interfacing with a remote terminal 102 for requesting access to computer network 104 (Figure 1). User 101 inserts authentication card 118 into card reader 116 thus providing the appropriate credentials associated with user 101 to remote terminal 102 for use in verification by

network server 108. In the preferred embodiment, remote terminal 102 performs a card interrogation 510 of card reader 116. Those skilled in the art will recognize that card reader 116 may interface with remote terminal 102 using established standard interfaces such as PCMCIA, serial bus, or other standard interfacing techniques. Card reader 116 then performs the appropriate interfacing to authentication card 118 over interface 114 (Figure 4).

Card reader 116 in response to card interrogation 510 receives a mobile subscriber identifier and authentication key in a response 512 from authentication card 118. In the preferred embodiment, authentication card 118 divulges the authentication key in addition to the mobile subscriber identifier. In an alternative embodiment of the present invention, authentication card 118 retains the authentication encryption key therein with encryption being preformed by the authentication card by the internally secure authentication key. In such an embodiment, information for encryption is presented to authentication card 118 wherein encryption is performed by the authentication key in conjunction with stored algorithms and the encrypted information is then returned. In the preferred embodiment, a computer data base 103 resident within remote terminal 102 retains the mobile subscriber identifier and the authentication key for subsequent use by remote terminal 102 during the authentication process. Remote terminal 102 retrieves the mobile subscriber identifier in a response 514. Remote terminal 102 initiates contact with network server 108 by performing dial up function 516.

Wireless modem 110 then cooperatively generates an unencrypted link 518 with network server 108. Network server 108 performing its firewall or protective function initiates a user identification request 520 to remote terminal 102. In response to user identification request 520, remote terminal 102 responds with a user identification response 522 comprised of the mobile subscriber unit identifier as previously retrieved from user authentication card 118.

Network server 108 upon receipt of the mobile subscriber identifier performs a verification step 524 wherein the mobile subscriber identifier is compared against the previously established authentication database 208. Population of authentication database 208 describing the preferred embodiment was previously described in Figure 2. Upon completion of the verification of the mobile subscriber identifier, network server 108, in the preferred embodiment, generates a random or pseudo-random number to initiate the authentication process.

In an alternative embodiment, as described in Figure 3, network server 108 may have had a random number previously established and distributed thereto. In such an

embodiment, subsequent authentication processes reuse the same random number to seed or initiate the authentication process.

Referring back to the preferred embodiment, network server 108 transmits a network authentication request 526 comprising the random number previously generated by network server 108. Remote terminal 102 upon receiving network authentication request 526 retrieves in a response 528 the authentication encryption key from computer database 103 in a response 528. Remote terminal 102, employing the authentication encryption key in conjunction with resident encryption algorithms, encrypts the received random number. As described above, in an alternative embodiment where authentication card 118 does not divulge the authentication encryption key, the random number is forwarded to the authentication card for performing encryption services. In such an embodiment, authentication card 118 then returns the encrypted random number through the card reader to remote terminal 102.

Remote terminal 102 generates an authentication response 530 comprised of the random number previously generated and transmitted by network server 108 encrypted by the authentication key originating from authentication card 118. Upon receipt of authentication response 530, network server 108 retrieves in a response 532 an authentication encryption key corresponding to the previously received mobile subscriber identifier. Network server 108 then encrypts the random number previously generated using this authentication encryption key in conjunction with resident encryption algorithms.

If user 101 of authentication card 118 is indeed an authorized user, then the authentication encryption key presented in authentication card 118 when used to encrypt the random number, will generate the same resultant encrypted random value as was generated by network server 108 when encrypting using its authentication key. Network server 108 then compares the encrypted random number as received in authentication response 530 with its resident generated encrypted random number.

In an alternative embodiment, network server 108 (Figure 3) retrieves the pre-computed authentication response 304 (Figure 3) for comparison with authentication response 530. When both results are equivalent, network server 108 has authenticated user 101 of remote terminal 102 as being an authorized user. Remote terminal 102, however, has not verified network 108 as being authentic. To facilitate this bi-directional process, network server 108 generates a mobile authentication response 534. Mobile authentication response 534 is comprised of the authentication response 530 as received from remote terminal 102 yet further encrypted by the authentication encryption key resident in network server 108. In an alternative embodiment, network server 108

(Figure 3) retrieves mobile authentication response 306 (Figure 3) for transmission to remote terminal 102. Such an encrypted response when received by remote terminal 102 demonstrates the authenticity of network server 108.

Remote terminal 102, upon receipt of mobile authentication response 534, internally encrypts the value previously generated for authentication response 530 for comparison with mobile authentication response 534, thus authenticating network server 108. Remote terminal 102 as operated by user 101 possessing an authentication card 118 has, therefore, been authenticated as being an authorized user of computer network 104 (Figure 1). Network server 108 proceeds to facilitate access by remote terminal 102 to computer network 104 (Figure 1).

To establish an encrypted link between remote terminal 102 and network server 108, each side must establish or generate a compatible data encryption key. Remote terminal 102 generates a data encryption key by encrypting its internally generated version of mobile authentication response 534. Likewise, network server 108 further encrypts mobile authentication response 534 using its authentication encryption key to generate a data encryption key. In an alternative embodiment, network server '108' (Figure 3) retrieves data encryption key 308 (Figure 3) for use in encrypting subsequent data.

In the preferred embodiment, remote terminal 102 transfers in response 536 the data encryption key it established to wireless modem 110. Wireless modem 110 then performs the encryption on subsequent data transmitted between remote terminal 102 and network server 108. In an alternative embodiment, remote terminal 102 retains the data encryption key and performs encryption of the data therein. An encrypted link 538 is, therefore, established for transmitting data encrypted in the data encryption keys between remote terminal 102 and network server 108. Correspondingly, remote terminal 102 and network server 108 upon receipt of encrypted data employs the data encryption key for decrypting the encrypted data.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respect only as illustratively and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured is:

1. In a computer network permitting remote access by an authorized user of a remote terminal via a wireless modem, a method for authenticating said authorized user prior to permitting access to said computer network, said method comprising:

securely distributing an authentication key to a network server of said computer network and to an authentication card for said authorized user, said authentication key being associated with a mobile subscriber identifier designating said authorized user;

establishing an unencrypted wireless communication channel between said remote terminal and said network server via a wireless modem; and

authenticating said user of said remote terminal according to mutually exchanged encrypted values.

2. The method as recited in claim 1, wherein said step of distributing an authentication key further comprises the steps of:

identifying an authorized user with a mobile subscriber identifier;

generating an authentication key to associate with said mobile subscriber identifier;

securely distributing said authentication key with said mobile subscriber identifier to said network server within said computer network; and

programming said authentication key with said mobile subscriber identifier into an authentication card for said authorized user.

3. The method as recited in claim 2, wherein said step of establishing an unencrypted wireless communication channel further comprises the steps of:

contacting said network server via said wireless modem; and

transmitting said mobile subscriber identifier from said authentication card to said network server via said unencrypted wireless communication channel.

4. The method as recited in claim 1, wherein said step of authenticating said user further comprises the steps of:

corroborating said mobile subscriber identifier of said authentication card with said mobile subscriber identifier of said network server;

mutually exchanging independently encrypted values between said remote terminal and said network server via said unencrypted wireless communication channel; and

comparing exchanged encrypted values with expected values.

5. The method as recited in claim 4, wherein said step of exchanging independently encrypted values further comprises the steps of:

generating a random number at said network server;

transmitting said random number to said remote terminal via said unencrypted wireless communication channel;

encrypting said random number at said remote terminal to form a remote terminal signed response;

returning said remote terminal signed response to said network server via said unencrypted wireless communication channel;

encrypting said remote terminal signed response at said network server to from a network signed response; and

returning said network signed response to said remote terminal via said unencrypted wireless communication channel.

6. The method as recited in claim 5, wherein the step of comparing exchanged encrypted values further comprises the steps of:

verifying said remote terminal signed response received at said network server with an expected value; and

verifying said network server signed response at said remote terminal with an expected value.

7. In a computer network permitting remote access by an authorized user of a remote terminal via a wireless modem, a method for establishing a secure authenticated wireless communication channel, said method comprising:

securely distributing an authentication key to a network server of said computer network and to an authentication card for said authorized user, said authentication key being associated with a mobile subscriber identifier designating said authorized user;

establishing an unencrypted wireless communication channel between said remote terminal and said network server via a wireless modem;

authenticating said user of said remote terminal according to mutually exchanged encrypted values; and

transforming said unencrypted wireless communication channel into an encrypted authenticated wireless communication channel using a data encryption key derived from said mutually exchanged values.

8. The method as recited in claim 7, wherein said step of distributing an authentication key step comprises the steps of:

identifying an authorized user with a mobile subscriber identifier;

generating an authentication key to associate with said mobile subscriber identifier;

securely distributing said authentication key with said mobile subscriber identifier to said network server within said computer network; and

programming said authentication key with said mobile subscriber identifier into an authentication card for said authorized user.

9. The method as recited in claim 8, wherein said step of establishing an unencrypted wireless communication channel further comprises the steps of:

contacting said network server via said wireless modem; and

transmitting said mobile subscriber identifier form said authentication card to said network server.

10. The method as recited in claim 7, wherein said step of authenticating said user further comprises the steps of:

corroborating said mobile subscriber identifier of said authentication card with said mobile subscriber identifier of said network server;

mutually exchanging independently encrypted values between said remote terminal and said network server via said unencrypted wireless communication channel; and

comparing exchanged encrypted values with expected values.

11. The method as recited in claim 10, wherein said step of exchanging independently encrypted values further comprises the steps of:

generating a random number at said network server;

transmitting said random number to said remote terminal via said unencrypted wireless communication channel;

encrypting said random number at said remote terminal to form a remote terminal signed response;

returning said remote terminal signed response to said network server via said unencrypted wireless communication channel;

encrypting said remote terminal signed response at said network server to from a network signed response; and

returning said network signed response to said remote terminal via said unencrypted wireless communication channel.

12. The method as recited in claim 11, wherein said step of comparing exchanged encrypted values further comprises the steps of:

verifying said remote terminal signed response received at said network server with an expected value; and

verifying said network server signed response at said remote terminal with an expected value.

13. The method as recited in claim 12, wherein said step of transforming said unencrypted wireless communication channel into an encrypted authenticated wireless communication channel further comprises the steps of:

yet further encrypting said network server signed response at the network server to form a data encryption key;

yet further encrypting said network server signed response at the remote terminal to also form a data encryption key corresponding to said data encryption key formed by said network server;

securing future data transferred between said remote terminal and said network server using said data encryption key; and

permitting access of said remote terminal to said computer network via said network server.

14. The method as recited in claim 13, wherein said step of securing future data comprises the steps of:

downloading the data encryption key to the wireless modem; and

encrypting the data at the wireless modem.

15. In a computer network permitting remote access by an authorized user of a remote terminal via a wireless modem through a network server, a method of authenticating said authorized user prior to permitting access to said computer network, said method comprising:

receiving a mobile subscriber identifier and an authentication key from an authentication card associated with said remote terminal;

said remote terminal cooperatively establishing an unencrypted wireless communication channel via said wireless modem with said network server; and

authenticating said user of said remote terminal according to mutually exchanged encrypted values.

16. The method as recited in claim 15, wherein said step of establishing an unencrypted wireless communication channel further comprises:

said remote terminal initiating said wireless modem to contact said network server; and

transmitting said mobile subscriber identifier as received from said authentication card to said network server.

17. The method as recited in claim 16, wherein said step of authenticating said user further comprises:

when said mobile subscriber identifier transmitted by said remote terminal corresponds to said authorized user as known to said network server, receiving at said remote terminal a random number generated by said network server;

encrypting said random number using said authentication key to form a remote terminal signed response;

returning said remote terminal signed response to said network server via said wireless modem;

when said remote terminal signed response concurs with an expected value at said network server, receiving at said remote terminal a network signed response generated by said network server by encrypting said remote terminal signed response using said authentication key; and

verifying said network signed response at said remote terminal with an expected value.

18. The method as recited in claim 15, wherein said step of receiving a mobile subscriber identifier and an authentication key further comprises the steps of:

said remote terminal querying a card reader operably coupled to said remote terminal for receiving said authentication card; and

receiving said mobile subscriber identifier and said authentication key from said authentication card via said card reader.

19. The method as recited in claim 18, further comprising the step of collocating said card reader and said wireless modem.

20. The method as recited in claim 18, wherein said authentication card conforms to a GSM subscriber identification module (SIM) and said mobile subscriber identifier is an international mobile subscriber identifier (IMSI).

21. In a computer network allowing remote access, a system for authenticating an authorized user prior to authorizing access to said computer network, said system comprising:

an account generator capable of generating both an authentication key and a mobile subscriber identifier for identifying said authorized user;

an authentication card for securely receiving said authentication key and said mobile subscriber identifier;

a remote terminal for facilitating remote access to said computer network, said remote terminal also receiving said authentication key and said mobile subscriber identifier from said account generator for use in authenticating said authorized user by encrypting and verifying mutually exchanged values across an encrypted wireless communication channel;

a network server for also securely receiving said authentication key from said account generator and for authenticating said remote terminal by encrypting and verifying mutually exchanged values with said remote terminal prior to permitting access to said computer network; and

a wireless modem operably coupled to said remote terminal and wirelessly coupled to said network server for establishing said wireless communication channel therebetween.

22. The system as recited in claim 21, wherein said account generator further comprises:

a means for securely distributing said authentication key with said mobile subscriber identifier to said network server within said computer network; and

a means for programming said authentication key with said mobile subscriber identifier into said authentication card for said authorized user.

23. The system as recited in claim 21, wherein said authentication card conforms to a GSM subscriber identification module (SIM) and said mobile subscriber identifier sis an international mobile subscriber identifier(IMSI).

24. The system as recited in claim 21, wherein said system further comprises a card reader operably coupled to said remote terminal for receiving said authentication card and extracting both said mobile subscriber identifier and said authentication key from said authentication card.

25. In a computer network allowing remote access by an authorized user via a network server, an apparatus for establishing an encrypted authenticated wireless communication channel with said network server prior to permitting remote access to said computer network, said apparatus comprising:

a means for receiving a mobile subscriber identifier and an authentication key from an authentication card associated with said authorized user;

a means for cooperatively establishing an unencrypted wireless communication channel with said network server;

a means for authenticating said user of said remote terminal according to mutually exchanged encrypted values; and

a means for transforming said unencrypted wireless communication channel into said encrypted authenticated wireless communication channel.

26. The apparatus as recited in claim 25, wherein said means for establishing an unencrypted wireless communication channel comprises:

a wireless modem operably coupled to said apparatus and wirelessly coupled to said network server for facilitating the establishment of said unencrypted wireless communication channel;

a means for initiating said wireless modem to contact said network server; and

a means for transmitting said mobile subscriber identifier as received from said authentication card to said network server.

27. The apparatus as recited in claim 25, wherein said means for authenticating further comprises:

a means for receiving a random number generated by said network server when said mobile subscriber identifier transmitted by said apparatus corresponds to said authorized user as known to said network server;

a means for encrypting said random number using said authentication key to form a remote terminal signed response;

a means for returning said remote terminal signed response to said network server via said wireless modem;

a means for receiving a network signed response generated by said network server by encrypting said remote terminal signed response using said authentication key when said remote terminal signed response concurs with an expected value at said network server; and

a means for verifying said network signed response with an expected value.

28. The apparatus as recited in claim 25, wherein said means for transforming said unencrypted wireless communication channel into said secure authenticated wireless communication channel comprises means for yet further encrypting said network server signed response at said apparatus to form a data encryption key for use in encrypting all subsequent transferred data.

29. The apparatus as recited in claim 25, wherein said means for receiving a mobile subscriber identifier and an authentication key further comprises:

a means for querying a card reader operably coupled to said remote terminal for receiving said authentication card; and

a means for receiving said mobile subscriber identifier and said authentication key from said authentication card via said card reader.

30. The apparatus as recited in claim 29, wherein said card reader and said wireless modem are integrated.

31. The apparatus as recited in claim 29, wherein said authentication card conforms to a GSM subscriber identification module (SIM) and said mobile subscriber identifier is an international mobile subscriber identifier (IMSI).

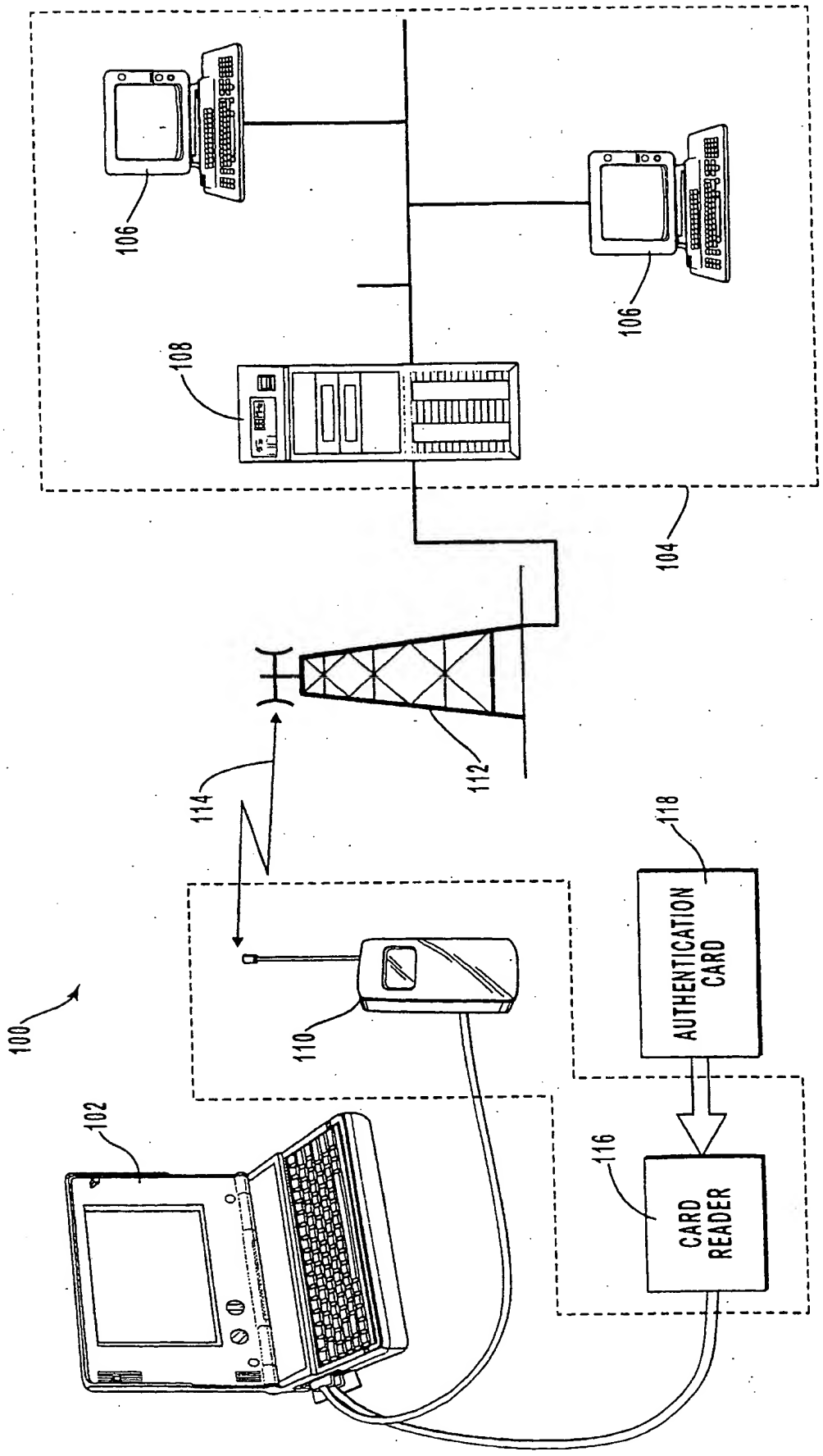

106
106
108
104
112
114
118
AUTHENTICATION CARD
110
100
102
116
CARD READER

FIG. 1

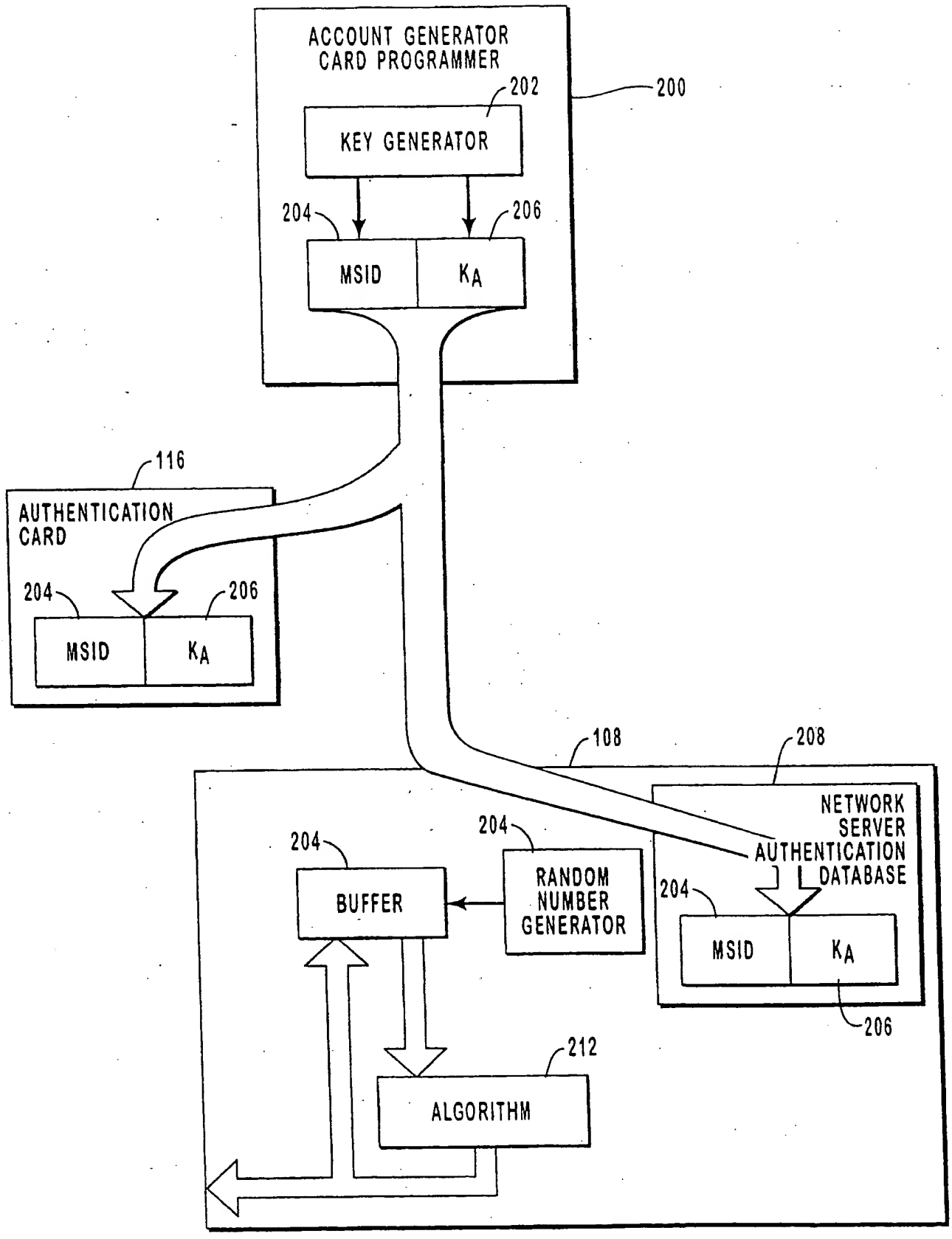

ACCOUNT GENERATOR CARD PROGRAMMER
200
202
KEY GENERATOR
204
206
MSID
KA
116
AUTHENTICATION CARD
204
206
MSID
KA
108
208
NETWORK SERVER AUTHENTICATION DATABASE
204
RANDOM NUMBER GENERATOR
204
BUFFER
204
MSID
KA
206
212
ALGORITHM

FIG. 2

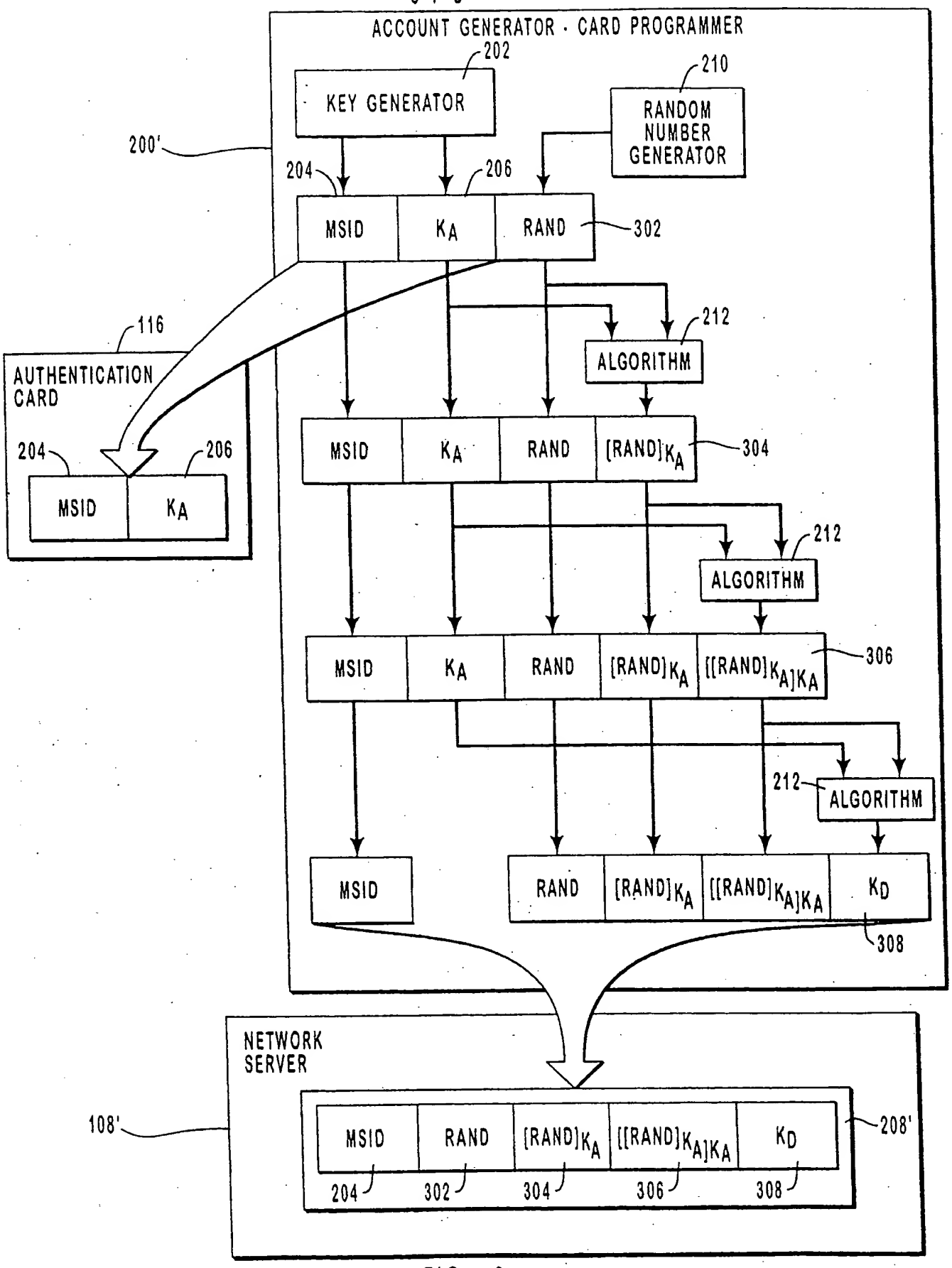

ACCOUNT GENERATOR · CARD PROGRAMMER
202
KEY GENERATOR
210
RANDOM NUMBER GENERATOR
200'
204
206
MSID
KA
RAND
302
116
AUTHENTICATION CARD
212
ALGORITHM
MSID
KA
RAND
[RAND]KA
304
212
ALGORITHM
MSID
KA
RAND
[RAND]KA
[[RAND]KA]KA
306
212
ALGORITHM
MSID
RAND
[RAND]KA
[[RAND]KA]KA
KD
308
NETWORK SERVER
108'
MSID
RAND
[RAND]KA
[[RAND]KA]KA
KD
208'
204
302
304
306
308

FIG. 3

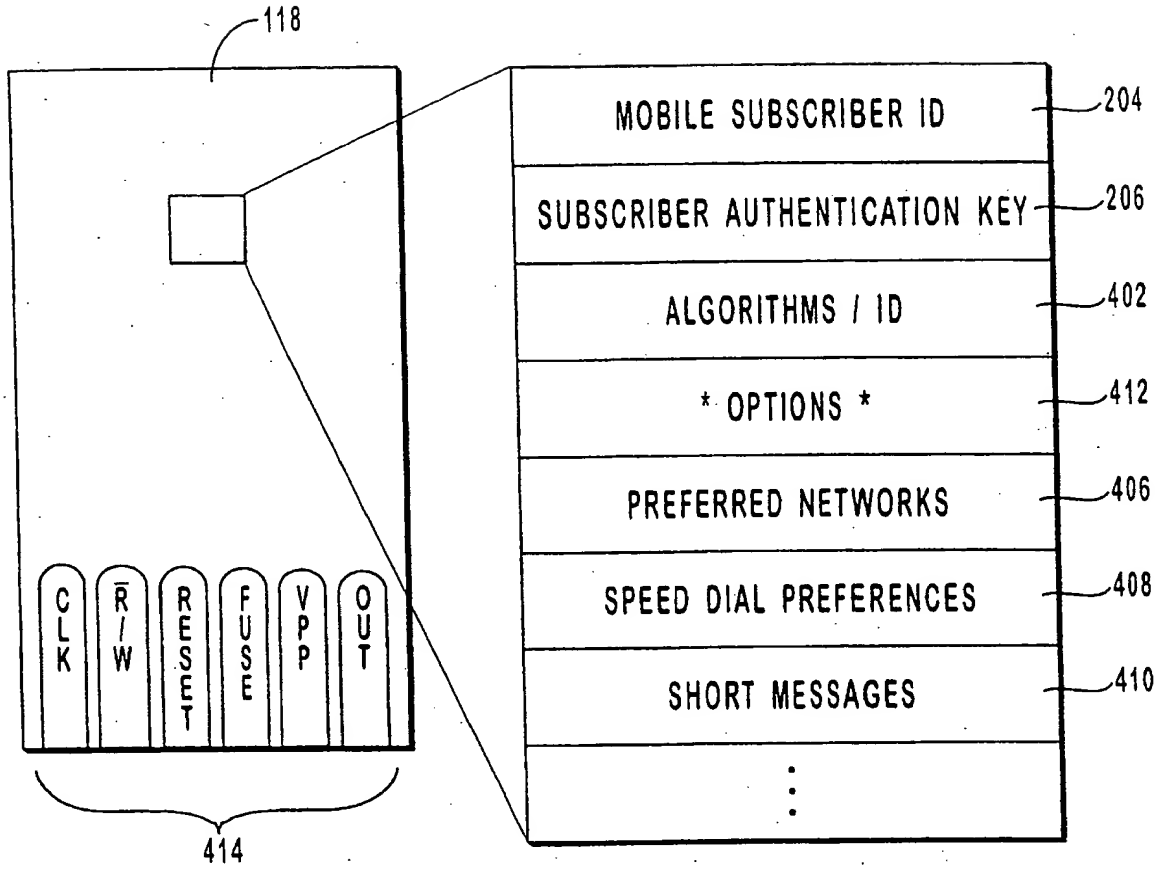

118
MOBILE SUBSCRIBER ID
204
SUBSCRIBER AUTHENTICATION KEY
206
ALGORITHMS / ID
402
* OPTIONS *
412
PREFERRED NETWORKS
406
SPEED DIAL PREFERENCES
408
SHORT MESSAGES
410
CLK
R/W
RESET
FUSE
VPP
OUT
414

FIG. 4

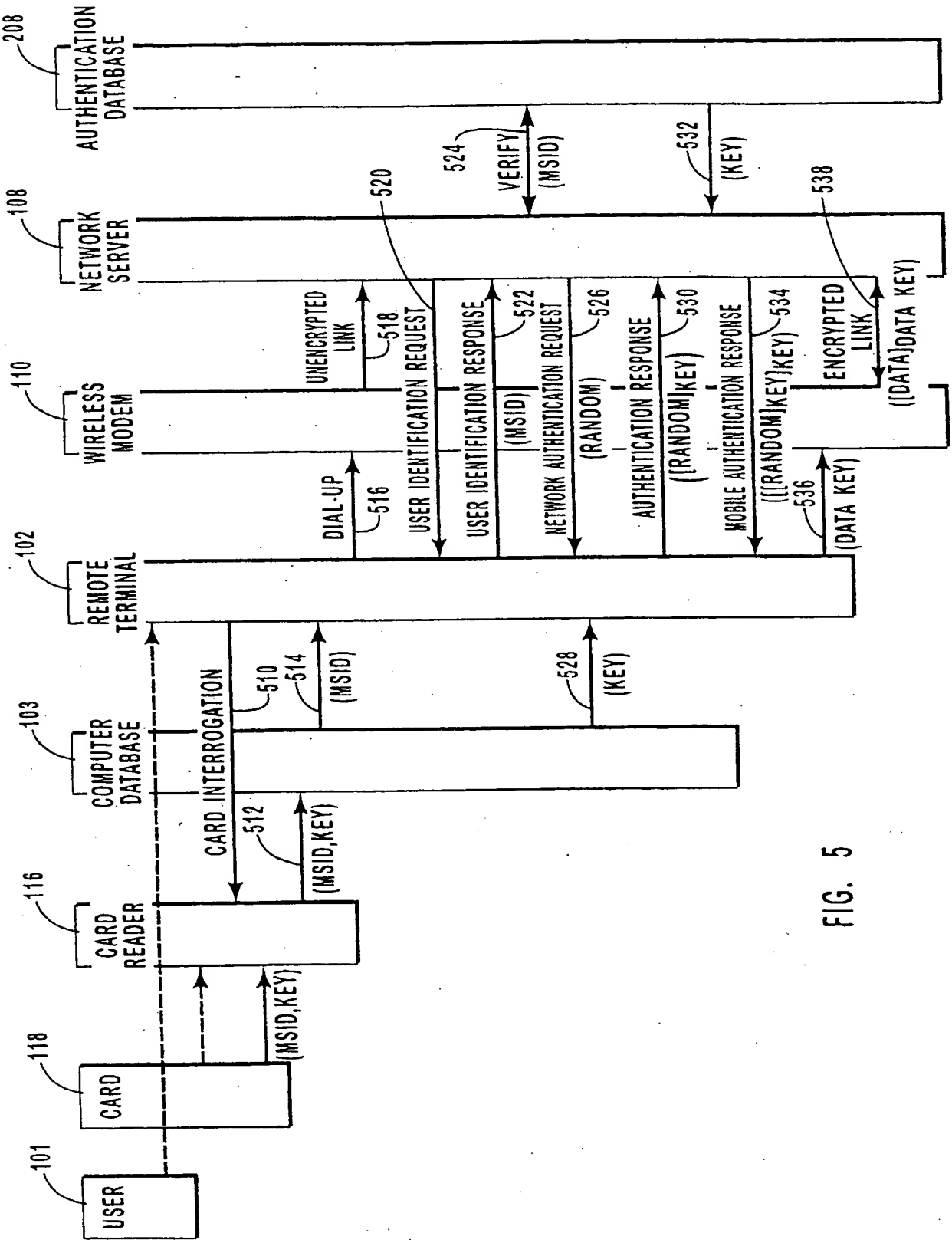

208
AUTHENTICATION DATABASE
108
NETWORK SERVER
110
WIRELESS MODEM
102
REMOTE TERMINAL
103
COMPUTER DATABASE
116
CARD READER
118
CARD
101
USER
CARD INTERROGATION
512
(MSID,KEY)
510
514
(MSID)
528
(KEY)
DIAL-UP
516
UNENCRYPTED LINK
518
520
USER IDENTIFICATION REQUEST
USER IDENTIFICATION RESPONSE
(MSID)
522
NETWORK AUTHENTICATION REQUEST
(RANDOM)
526
AUTHENTICATION RESPONSE
([RANDOM]KEY)
530
MOBILE AUTHENTICATION RESPONSE
(([RANDOM]KEY)KEY)
534
536
(DATA KEY)
ENCRYPTED LINK
538
((DATA]DATA KEY)
524
VERIFY
(MSID)
532
(KEY)

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/02839

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00, 9/08
US Cl. 380/25, 21, 49
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25, 21, 49; 395/187.01, 188.01

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS searc terms: mutual authentication, gateway, network server, authentication key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 5,602,918 A (CHEN et al.) 11 February 1997 - see entire document.	1-12,15-19, 21, 22, 24-27, 29, and 30 ---- 20, 23 & 31
Y,E	US 5,740,361 A (BROWN) 14 April 1998 - see entire document.	1-4, 7-10
Y, E	US 5,742,756 A (DILLAWAY et al.) 21 April 1998 - column 3 lines 6-45).	1-4, 7-10
Y	US 5,557,679 A (JULIN et al.) 17 September 1996 - see entire document.	20, 23, and 31

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 26 MAY 1998	Date of mailing of the international search report 25 JUN 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PINCHUS M.LAUFER Telephone No. (703) 306-4177

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/02839

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,351,293 A (MICHENER et al.) 27 September 1994 - see entire document; see particularly Abstract and figure 1.	1-12, 15-27, and 29-31
A	US 5,588,059 A (CHANDOS et al.) 24 December 1996 - see entire document.	1-31